

FIG.1

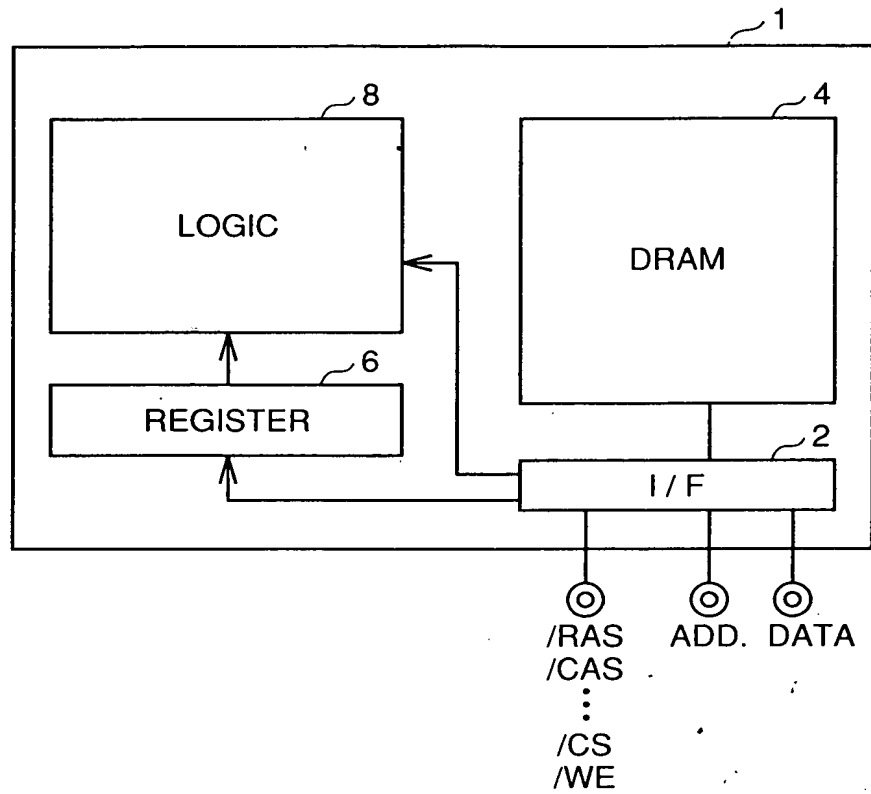


FIG.2

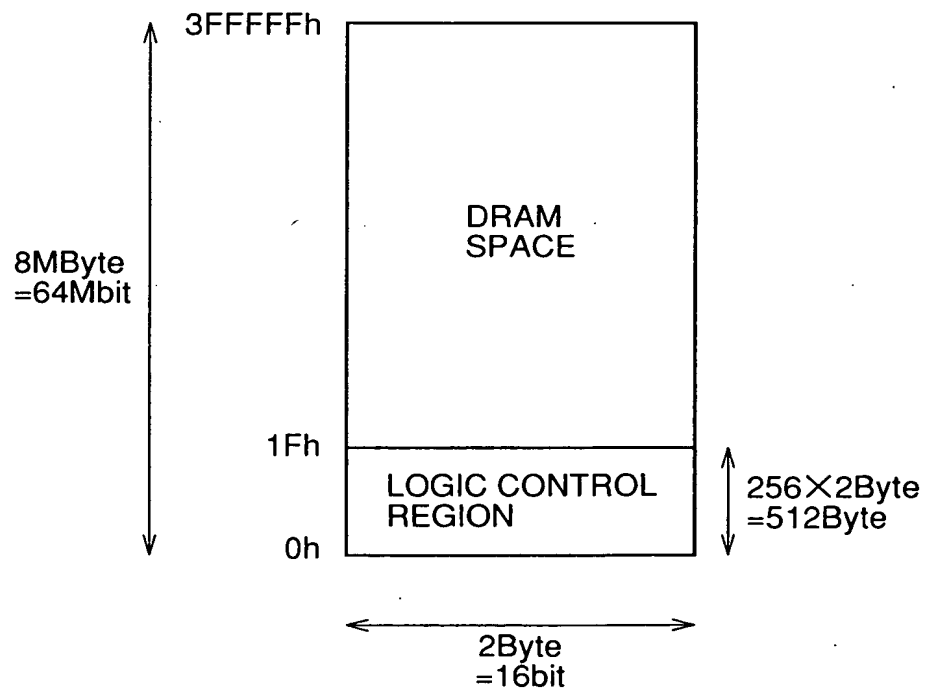


FIG.3

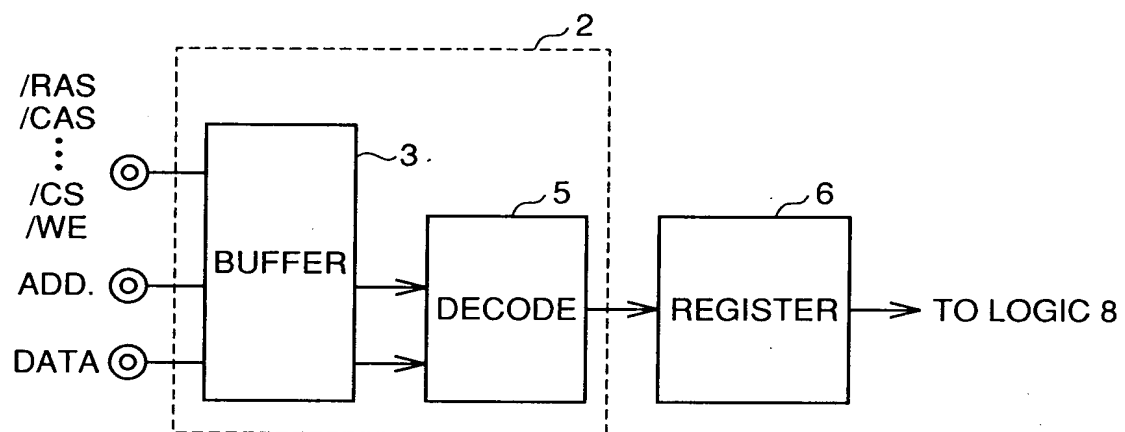


FIG.4

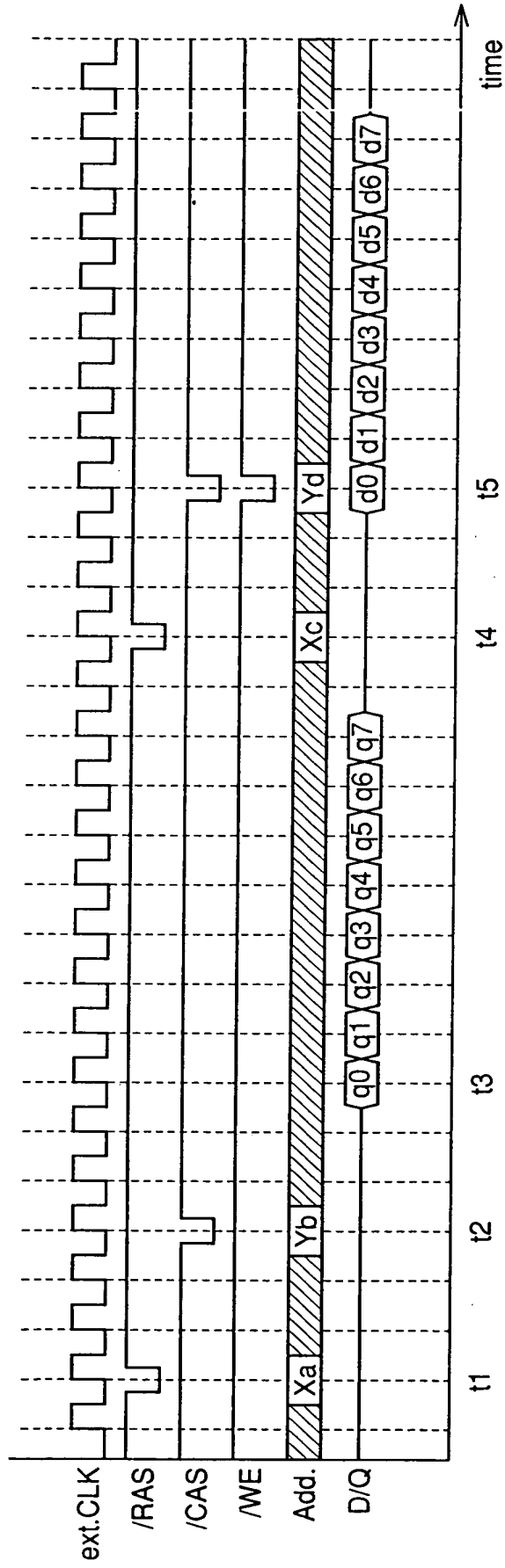


FIG.5

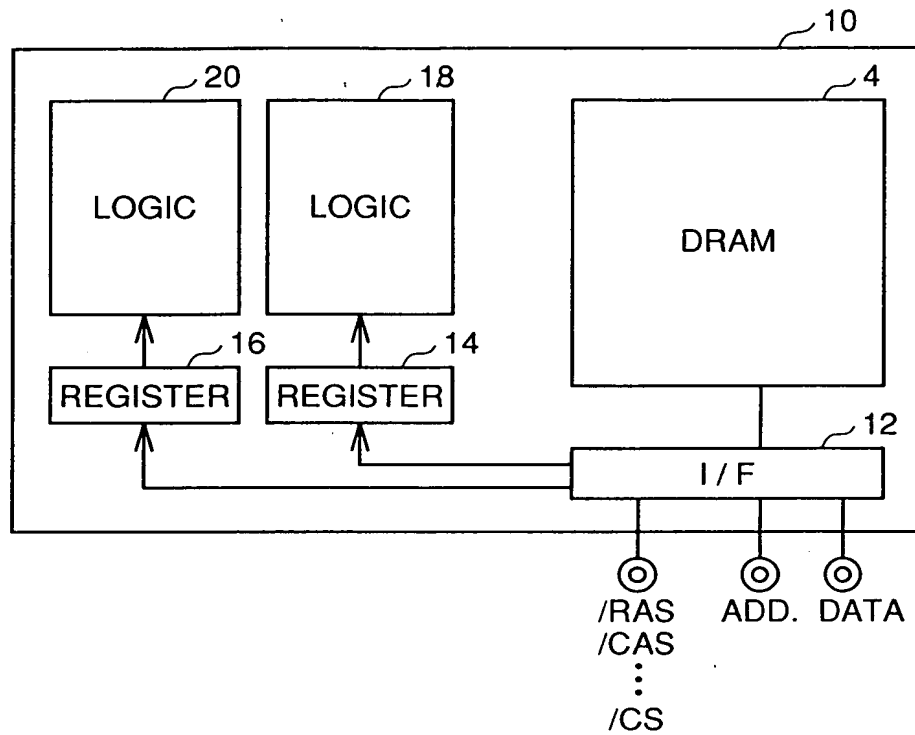


FIG.6

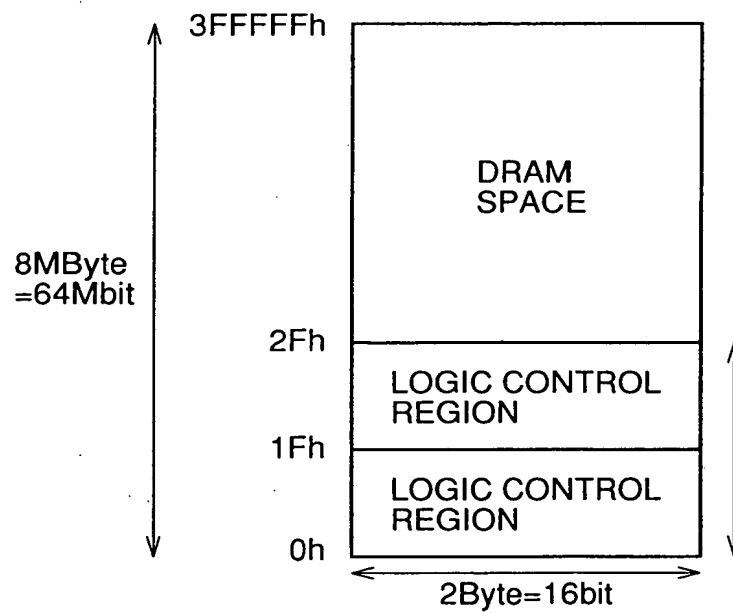


FIG. 7

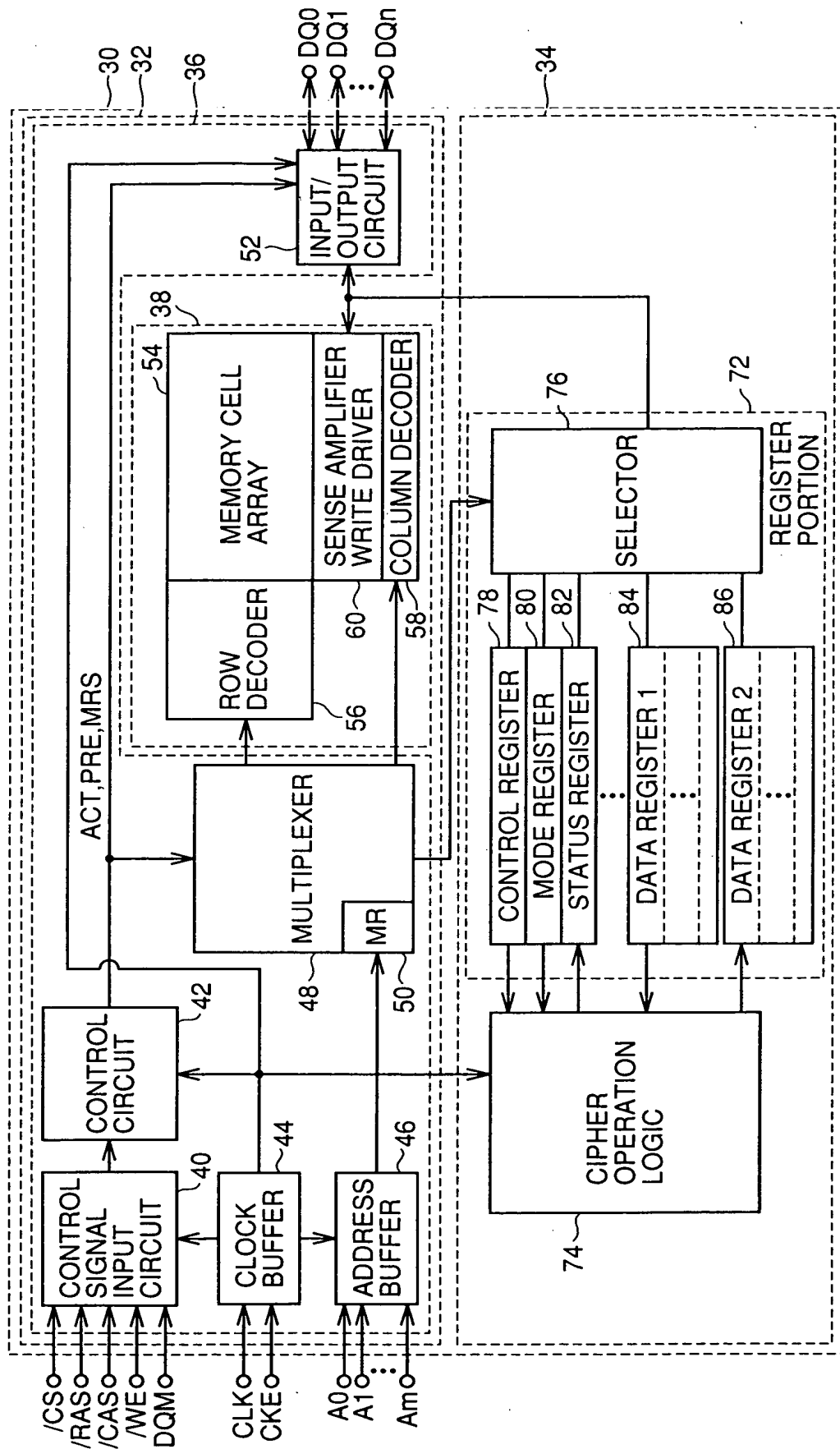


FIG.8

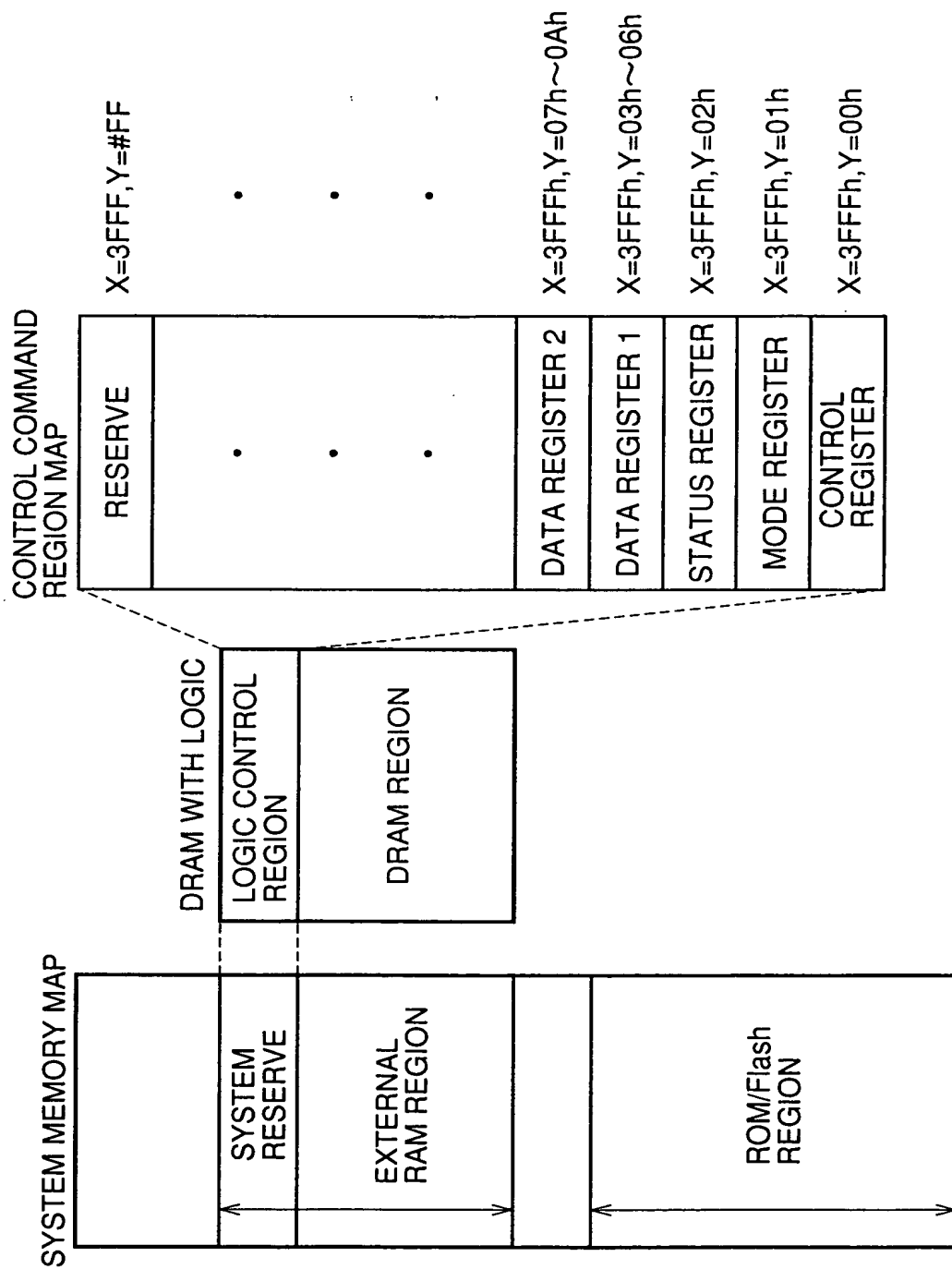


FIG.9

PUBLIC KEY CRYPTOSYSTEM	SECRET KEY CRYPTOSYSTEM	
RSA	DES Triple DES	BLOCK ENCRYPTION MODE
		ECB:Electric Code Book CBC:Cipher Block Chaining OFB:Output Feed Back CFB:Cipher Feed Back

SUPPORTED CRYPTOSYSTEMS

FIG.10

- BOTH FOR PUBLIC KEY AND SECRET KEY METHODS

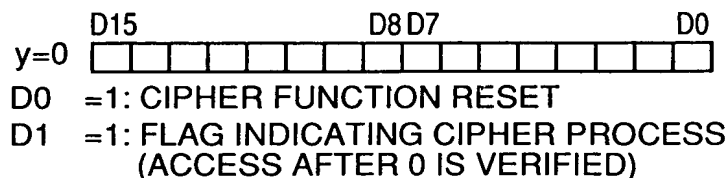


FIG.11

- CONTROL IN SECRET KEY METHOD

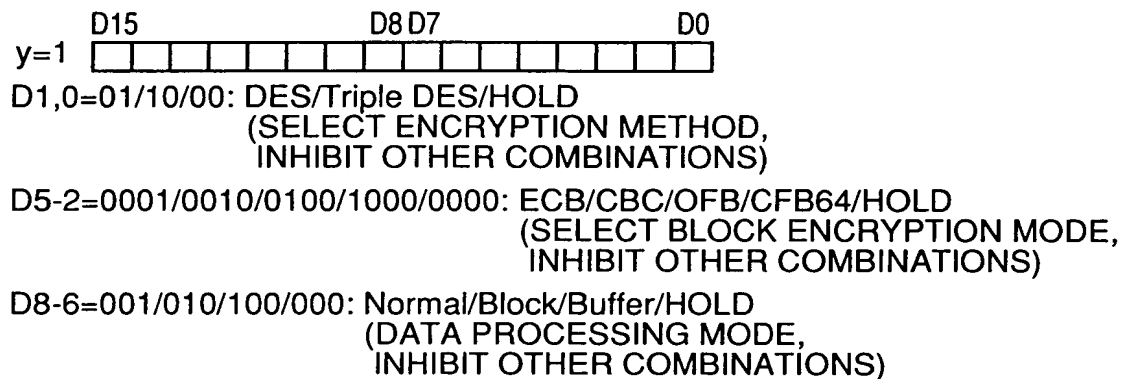


FIG.12

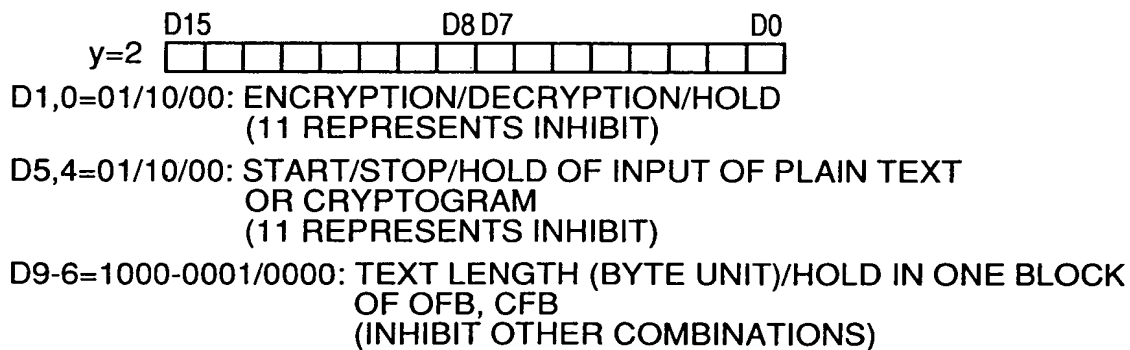


FIG.13

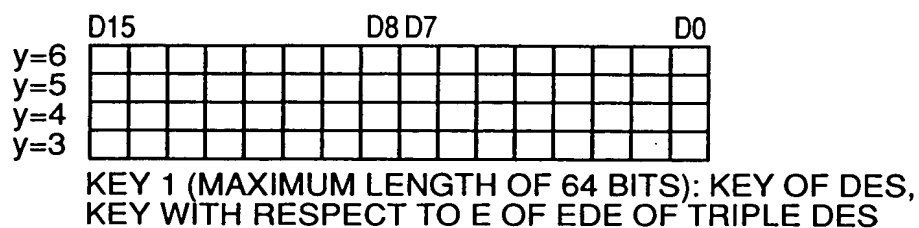


FIG.14

	D15				D8 D7				D0			
y=A												
y=9												
y=8												
y=7												

KEY 2 (MAXIMUM LENGTH OF 64 BITS):
KEY WITH RESPECT TO D OF EDE OF TRIPLE DES

FIG.15

	D15				D8 D7				D0			
y=E												
y=D												
y=C												
y=B												

IV: INITIAL VECTOR

FIG.16

	D15				D8 D7				D0			
y=F												

BLOCK LENGTH: SET BY BYTE UNIT
Max=2kByte(D=#FF) Min=1Byte(D=#0)

FIG.17

	D15				D8 D7				D0			
y=10												

BUFFER NUMBER: VALID IN BUFFER MODE
Max=64k(D=#FFFF) Min=1(D=#0)

FIG.18

	D15				D8 D7				D0			
y=11												

BUFFER ID:

FIG.19

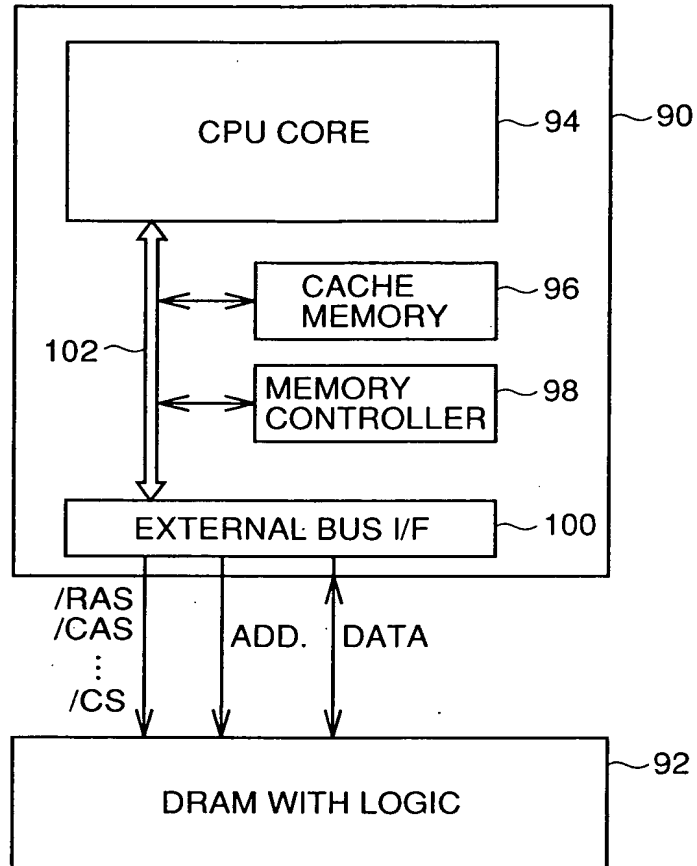


FIG.20

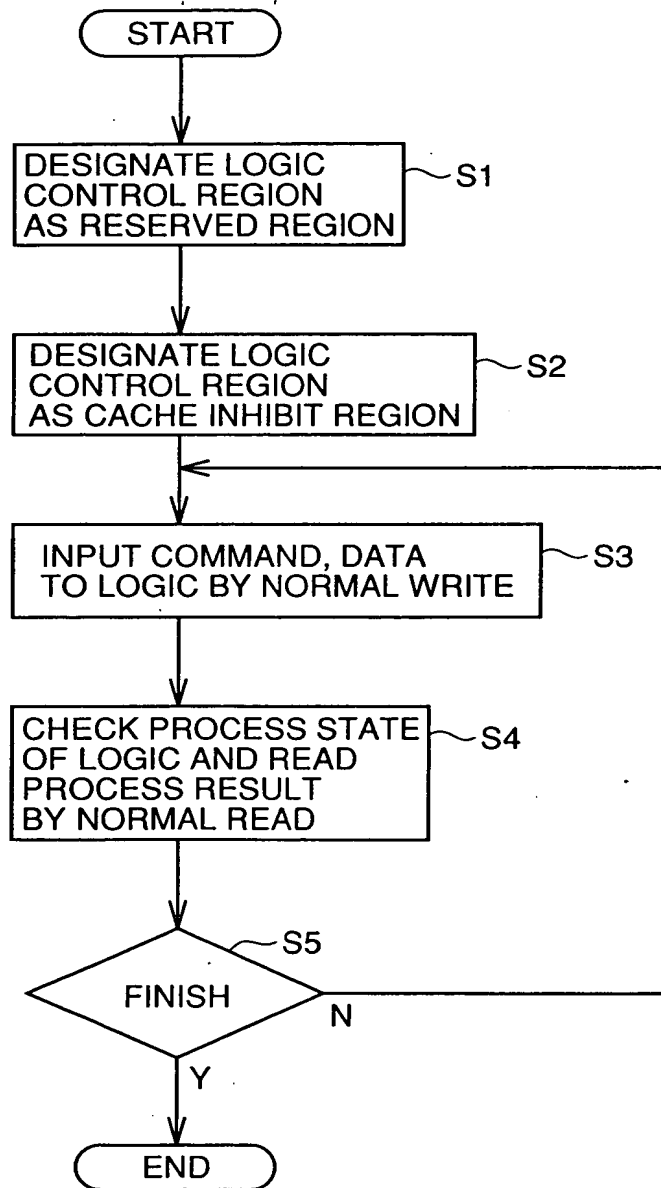


FIG.21

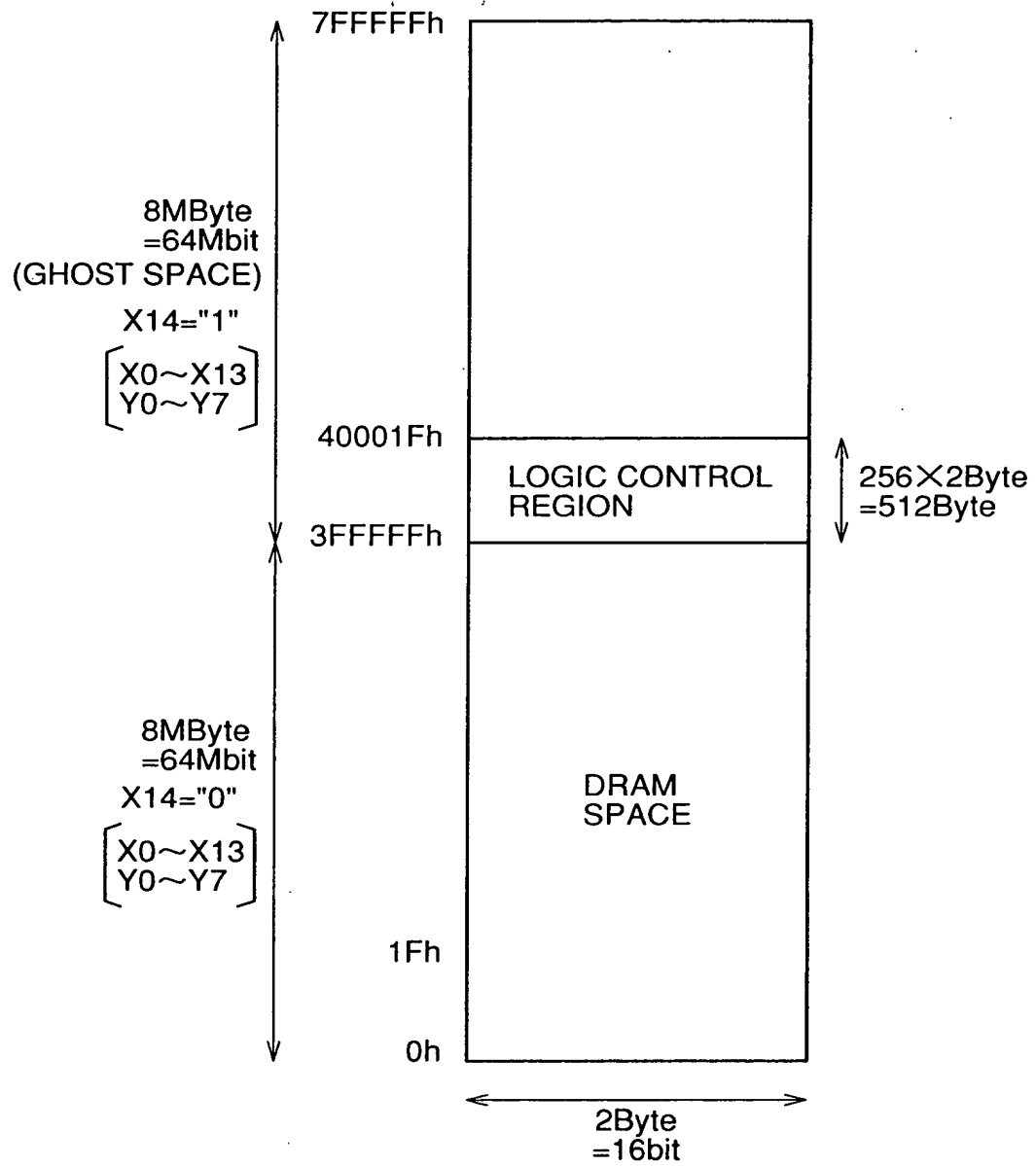


FIG.22

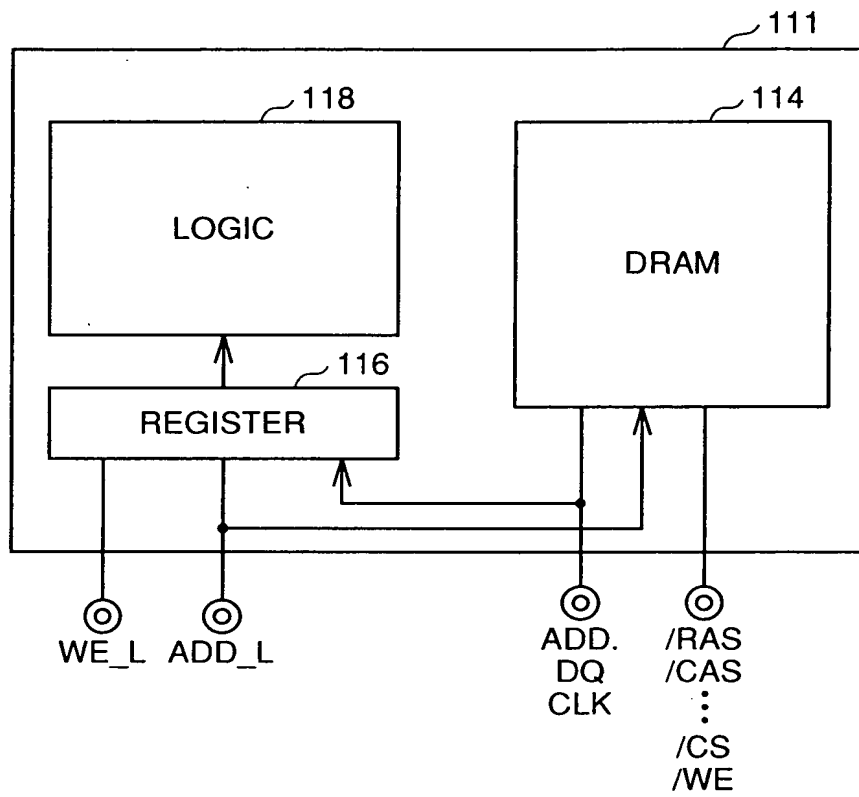


FIG.23

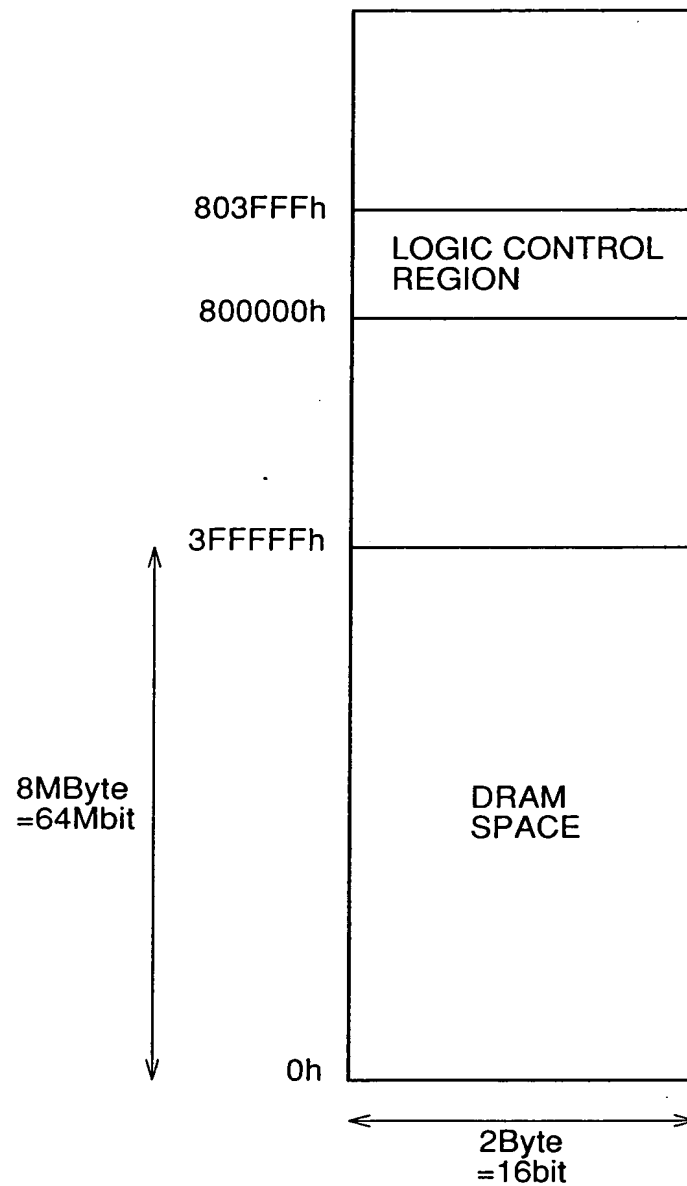


FIG.24

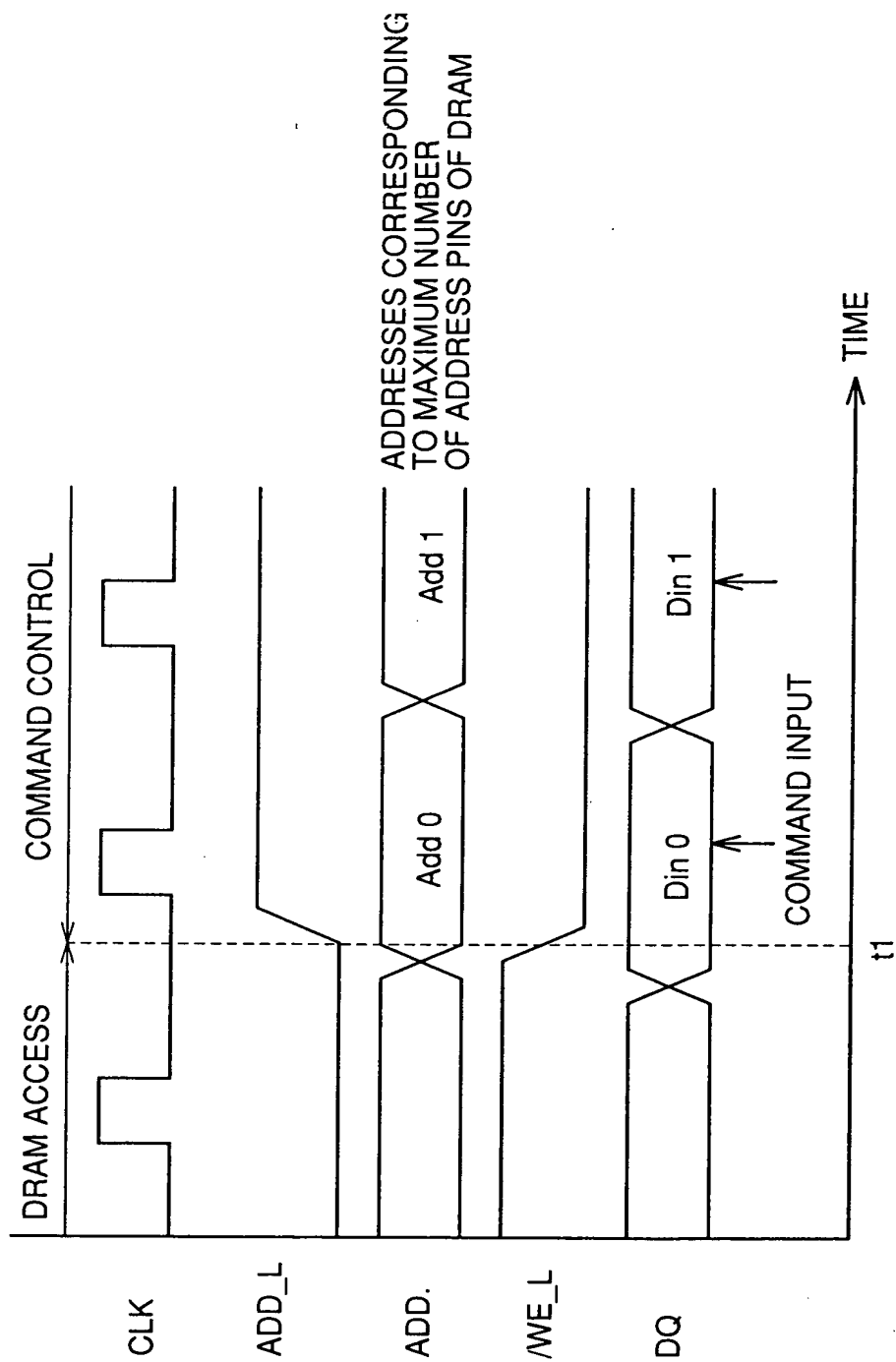


FIG.25

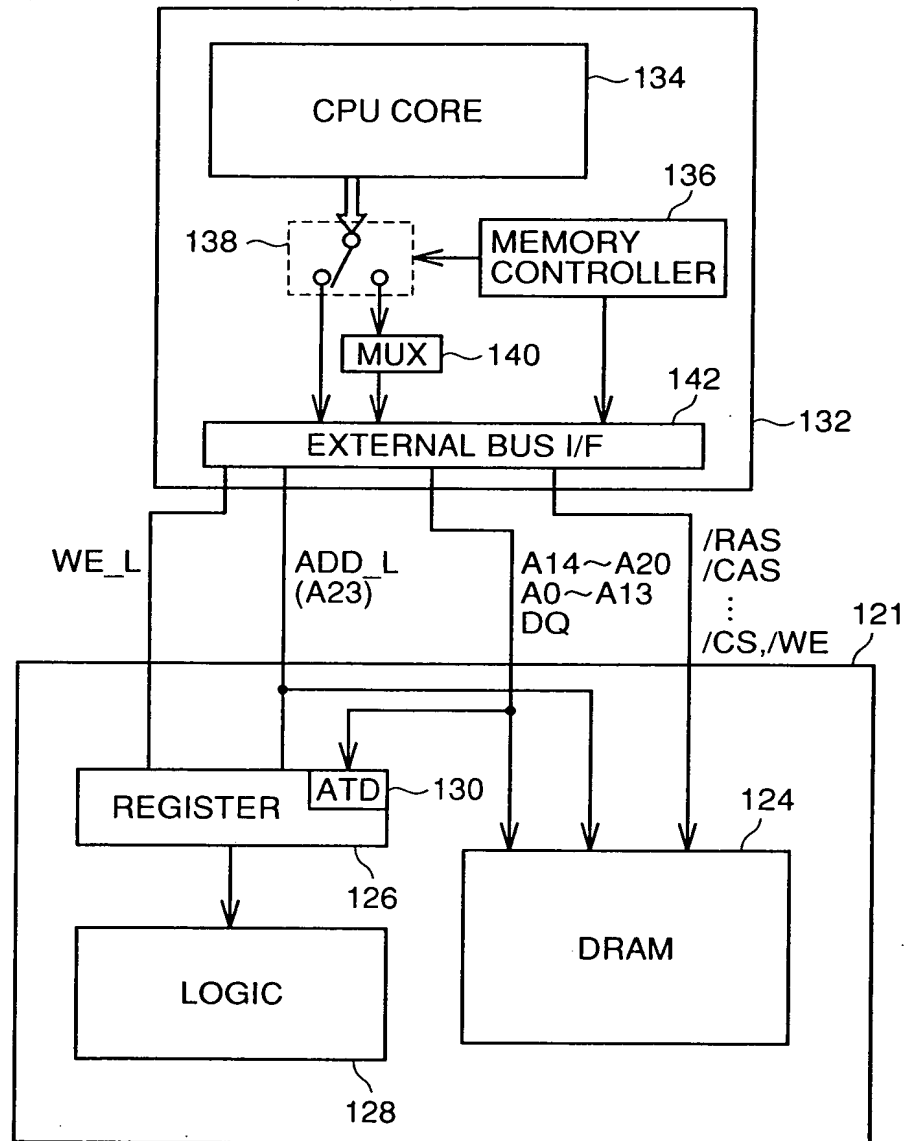


FIG.26

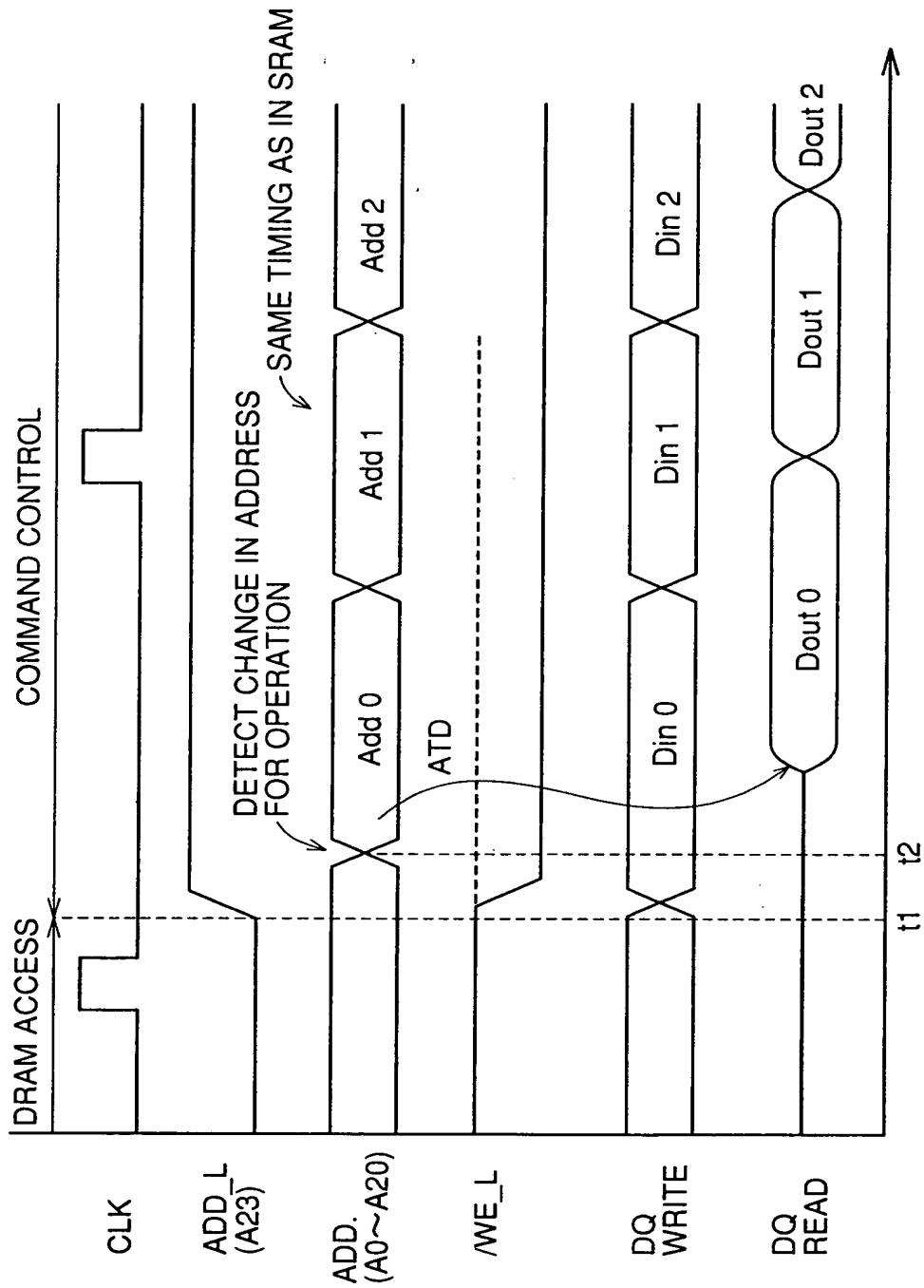


FIG.27

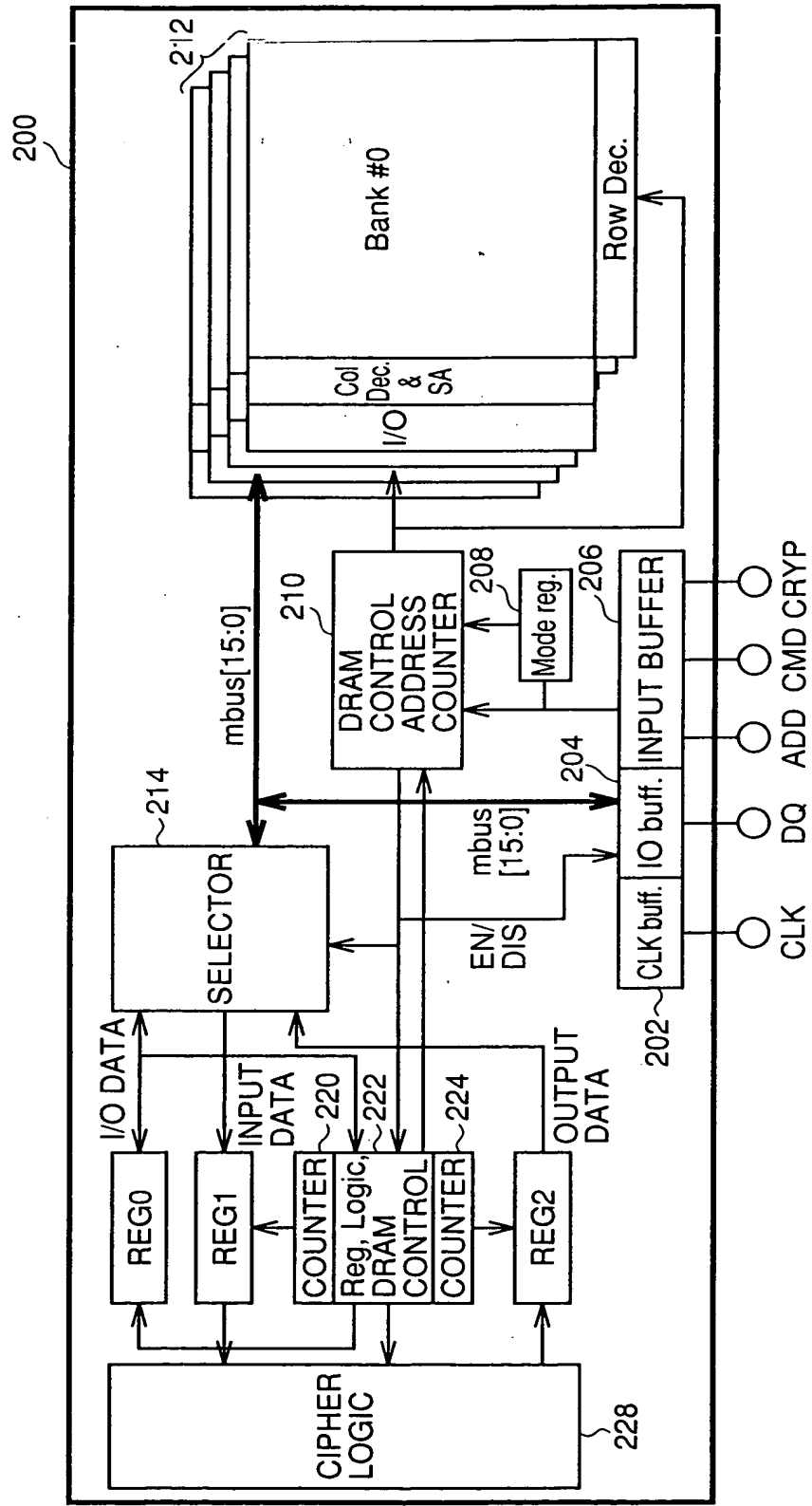


FIG.28

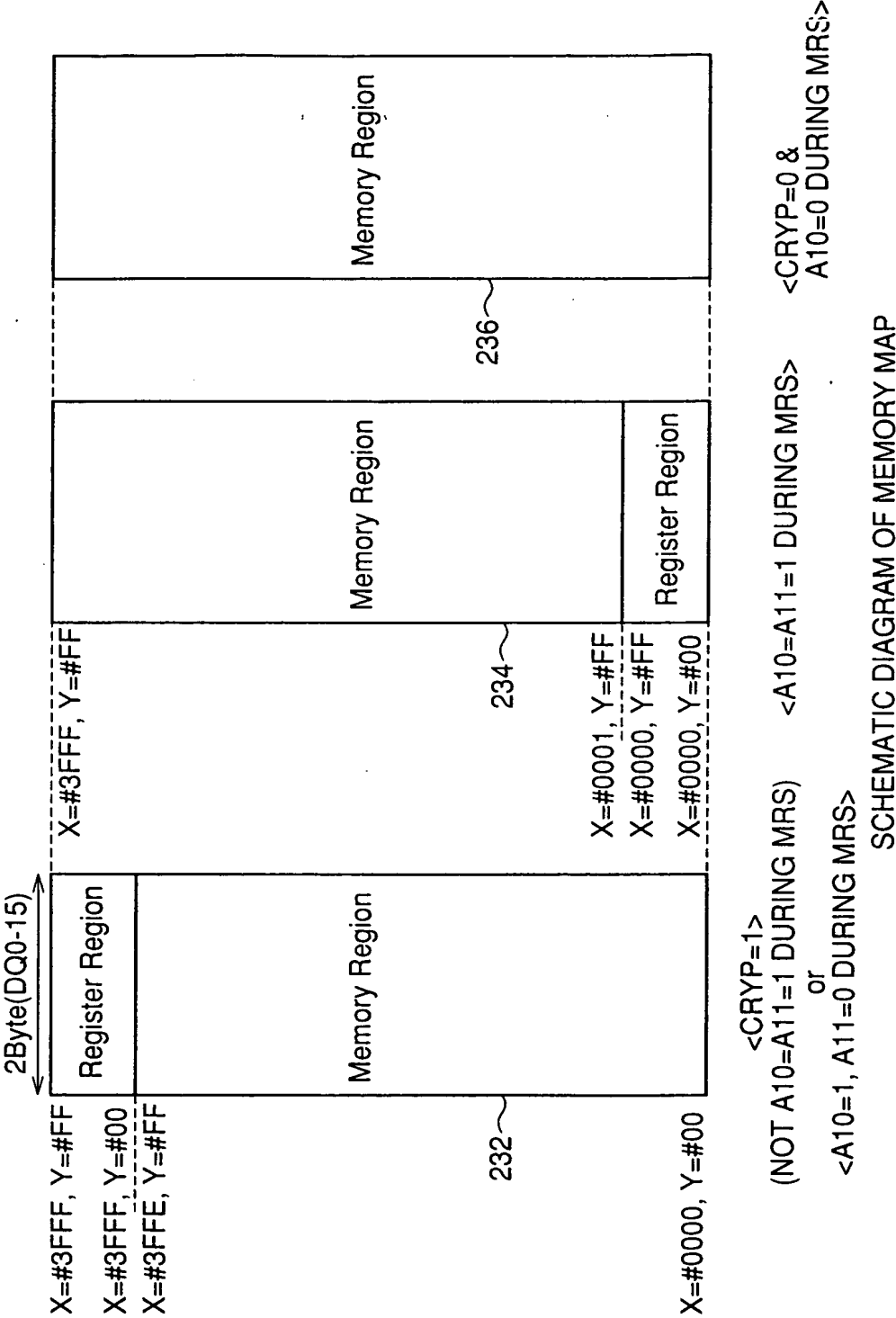


FIG.29

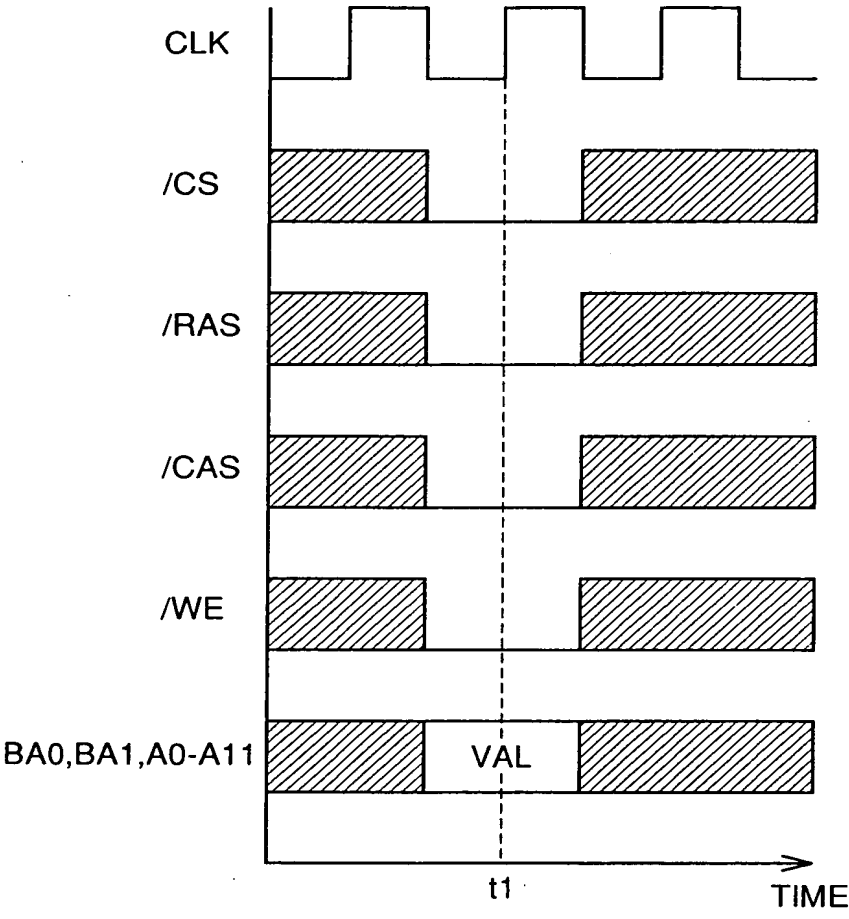


FIG.30

BA0	BA1	A11	A10	A9	A8	A7	A6	A5	A4	A3	A2	A1	A0
					0	0							

FIG.31

Bits	Name	Description	
A2..0	Burst Length	000	1
		001	2
		010	4
		011	8
		100	R
		101	R
		110	R
		111	Full Page
A3	Burst Type	0	Sequential
		1	Interleaved
A6..4	CAS Latency	000	R
		001	R
		010	2
		011	3
		1XX	R
A9	Write Mode	0	Burst
		1	Single Bit
A10	Control Reg. Access	0	Disable
		1	Enable
A11	Control Reg. Address	0	X=3FFF
		1	X=0
BA1	Low Power Mode	0	Disable
		1	Enable
BA0	Low Clock Frequency	0	Disable
		1	Enable

FIG.32

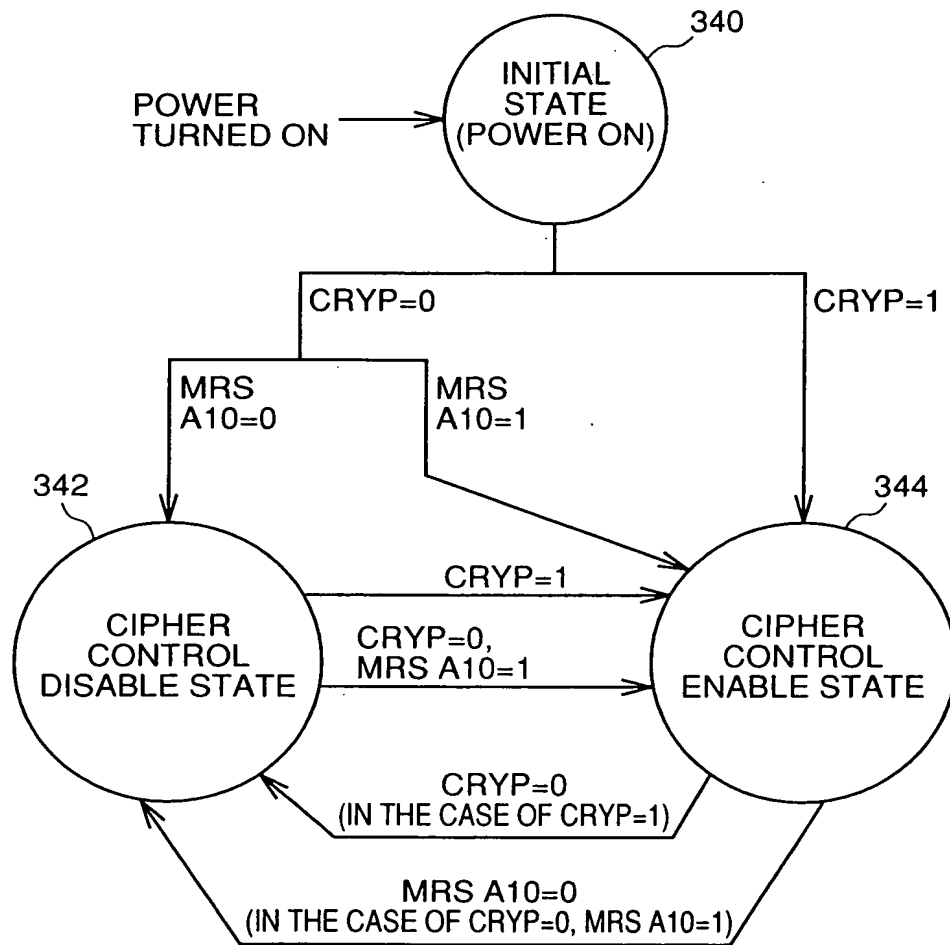


FIG.33

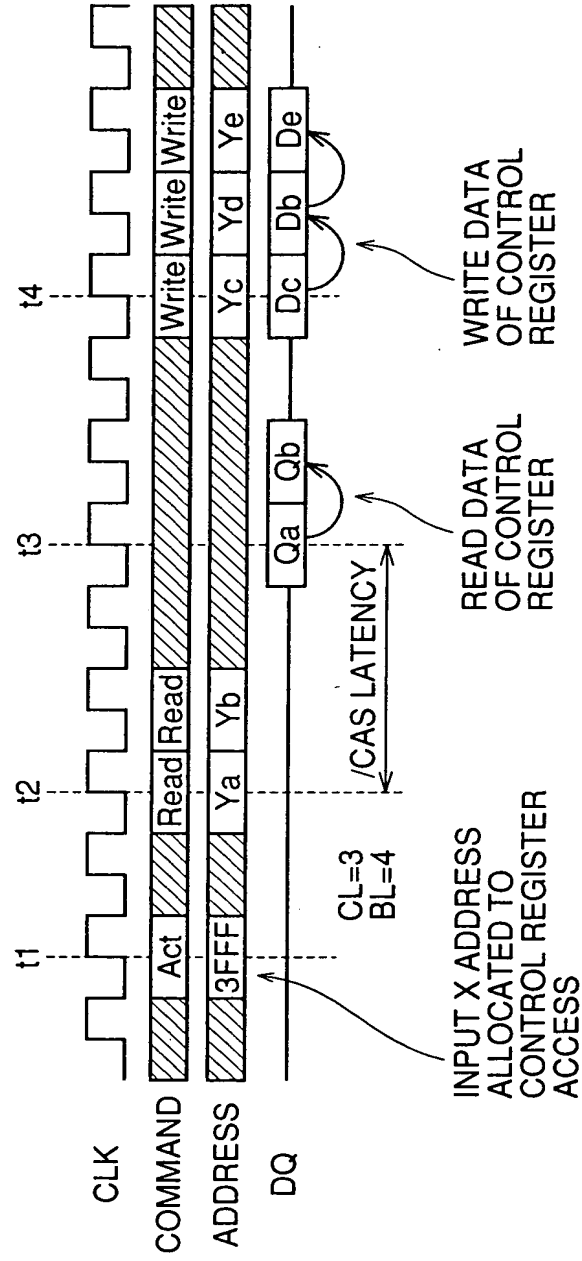


FIG.34

Col. Add.	Bits	Name	Description	Access
h00	D0	Software Reset	Reset	W
	D1	Flag	Done	R
			Processing	R
	D2	Change add for reg. cont.	X=h3FFF	W
	D3	Change add for reg. cont.	X=h0	W
	D4	EOF(End of File)		W
h01	D1	Partial Refresh	Bank0 Enable/Disable	W
	D2		Bank1 Enable/Disable	W
	D3		Bank2 Enable/Disable	W
	D4		Bank3 Enable/Disable	W
	D5	LP Mode	Enable/Disable	W
	D6	Low Clock Frequency	Enable/Disable	W

FIG.35

Col. Add.	Bits	Name	Description	Access
h02	D1..0	Secret Crypt. Mode	00 Hold	W
			01 DES-56	W
			10 Triple DES-112	W
			11 Triple DES-168	W
	D5..2	Block Crypt. Mode	0000 Hold	W
			0001 ECB	W
			0010 CBC	W
			0100 OFB	W
	D9..6	Enabled bank set in Reg-DRAM transfer mode	1000 CFB-64	W
			0000 All Bank Disable	W
			1/0 Bank0 Enable/Disable	W
			1/0 Bank1 Enable/Disable	W
			1/0 Bank2 Enable/Disable	W
			1/0 Bank3 Enable/Disable	W
	D10	Simultaneous transfer	1/0 Enable/Disable	W

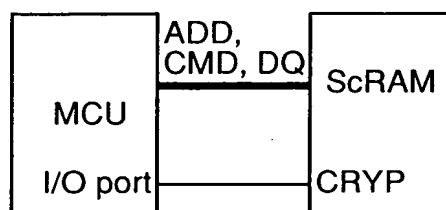
FIG.36

Col. Add.	Bits	Name	Description	Access
h03	D1..0	ENC/DEC	00 Hold	W
			01 Encryption	W
			10 Decryption	W
			11 RFU	W
	D2	Counter of reg1	Reset	W
	D3	Counter of reg2	Reset	W
	D4	IV Load	0 Previous output	W
			1 IV Load	W
	D8..5	Text length per block	0000 Hold	W
			Else (D8..5)x1Byte	W
h04	D15..0	Reg.1 Access	Write Data: D15..0	W
h05	D15..0	Reg.2 Access	Read Data: D15..0	R
h06	D0	Reg-DRAM transfer	Mode entry	W
	D1		Mode exit	W
	D2		Counter reset of reg1	W
	D3		Counter reset of reg1	W

FIG.37

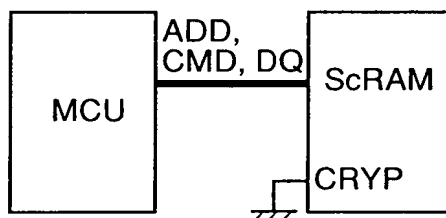
Col. Add.	Bits	Name	Description	Access
h13-h10	D15..0	Key1 for DES, Triple DES	LSB: h10[D0] USB: h13[D15] Key1 Input	W
h17-h14	D15..0	Key2 for Triple DES	LSB: h14[D0] USB: h17[D15] Key2 Input	W
h1B-h18	D15..0	Key3 for Triple DES-168	LSB: h18[D0] USB: h17B[D15] Key3 Input	W
h1F-h1C	D15..0	Initial Vector (IV)	LSB: h1C[D0] USB: h1F[D15] IV Input	W
hFF-h20	D15..0	Reserved		

FIG.38



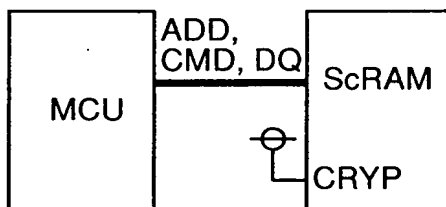
CONTROL CRYP TERMINAL BY I/O PORT

FIG.39



FIX CRYP TERMINAL AT L

FIG.40



FIX CRYP TERMINAL AT H

FIG.41

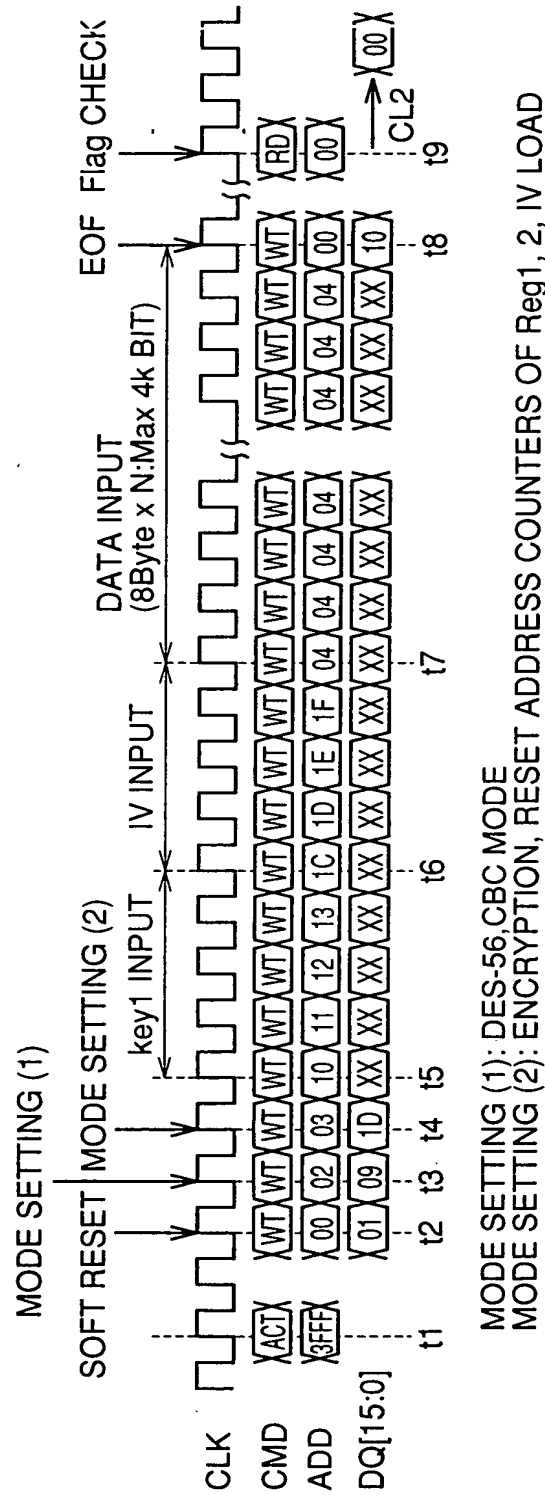


FIG.42

〈BASIC UNIT FOR ENCRYPTION PROCESS〉

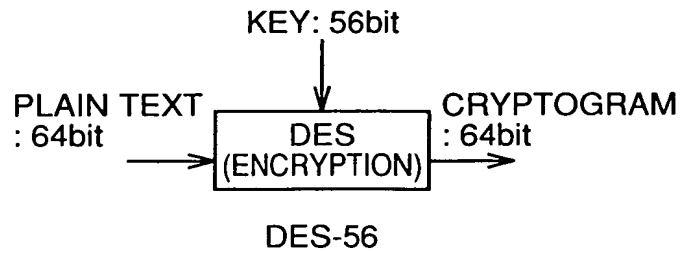


FIG.43

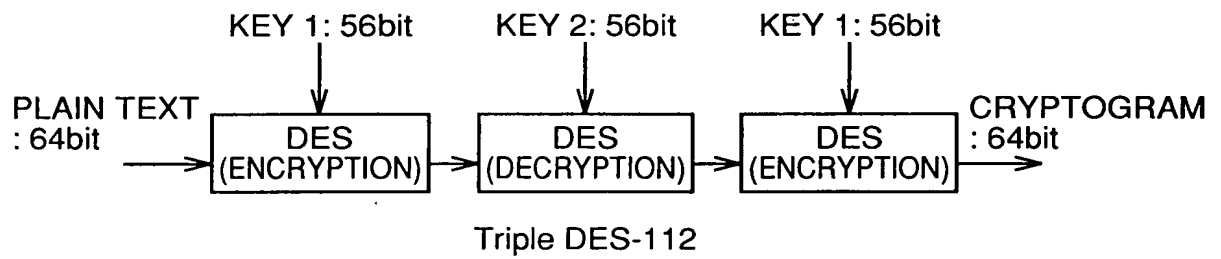


FIG.44

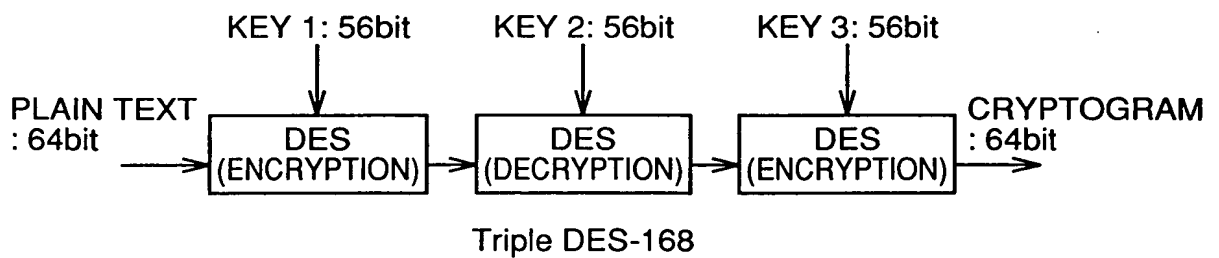


FIG.45

〈BASIC UNIT FOR DECRYPTION PROCESS〉

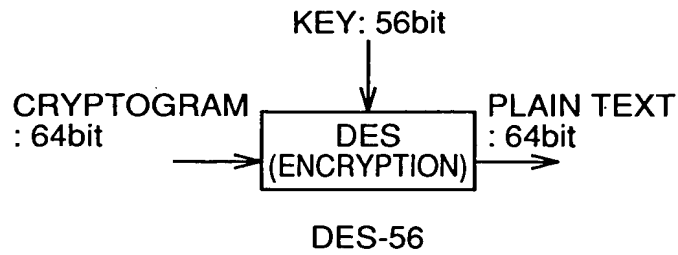


FIG.46

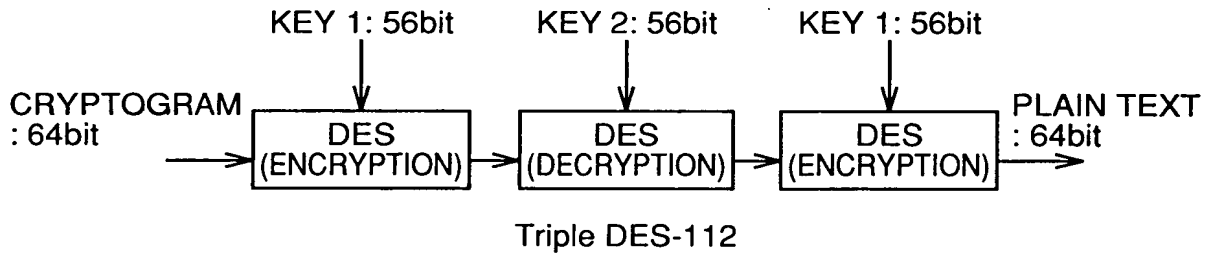


FIG.47

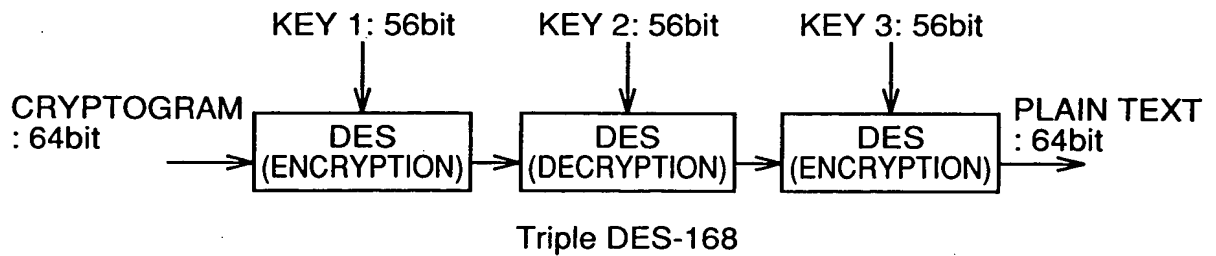


FIG.48

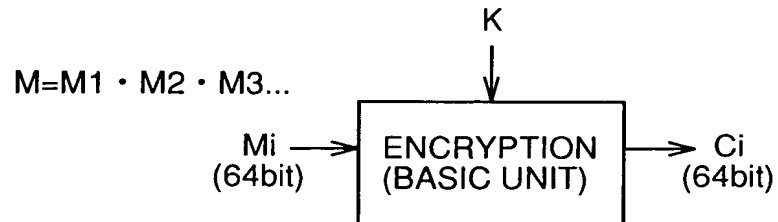


FIG.49

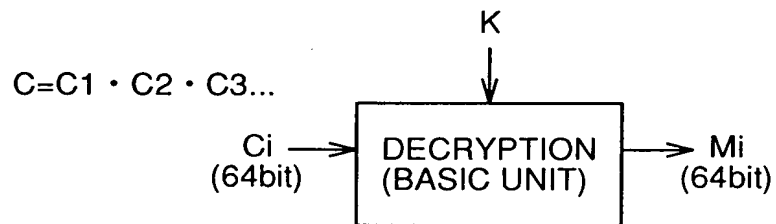
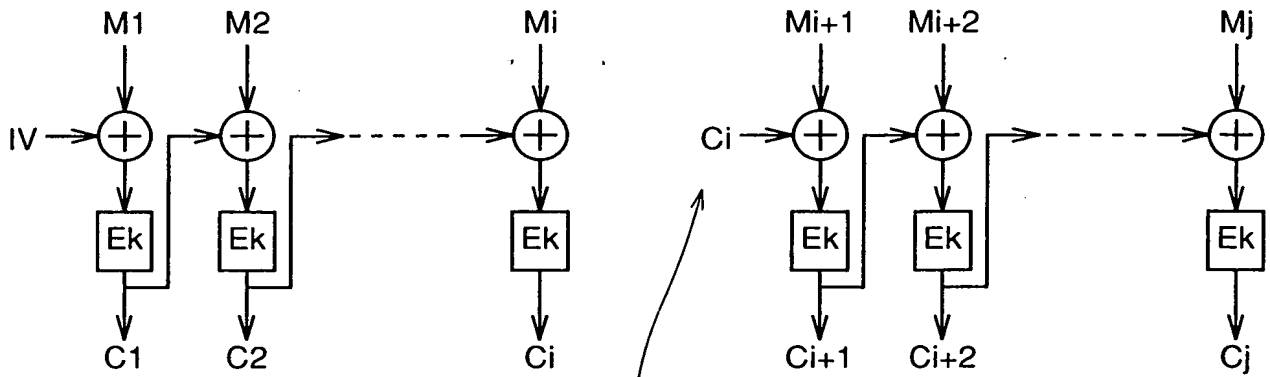


FIG.50

$$\begin{aligned}
 C1 &= E_k (M1 \oplus IV) \\
 Ci &= E_k (Mi \oplus Ci-1) \quad (i=2,3,\dots) \\
 M1 &= D_k (C1) \oplus M1 \\
 Mi &= D_k (Ci) \oplus Ci-1 \quad (i=2,3,\dots)
 \end{aligned}$$

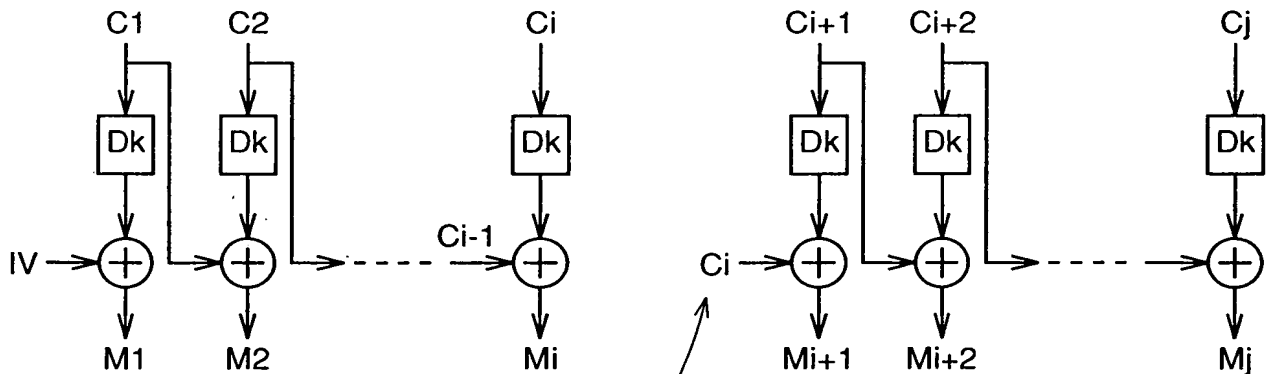
FIG.51



MAKE INITIAL VALUE CORRESPOND
TO CRYPTOGRAM C_i IMMEDIATELY
BEFORE IF PLAIN TEXT M IS LONGER
THAN REGISTER 1

〈SCHEMATIC DIAGRAM OF ENCRYPTION IN CBC MODE〉

FIG.52



MAKE INITIAL VALUE CORRESPOND
TO ENCRYPTION TEXT C_i IMMEDIATELY
BEFORE IF PLAIN TEXT M IS LONGER
THAN REGISTER 1

〈SCHEMATIC DIAGRAM OF DECRYPTION IN CBC MODE〉

FIG.53 PRIOR ART

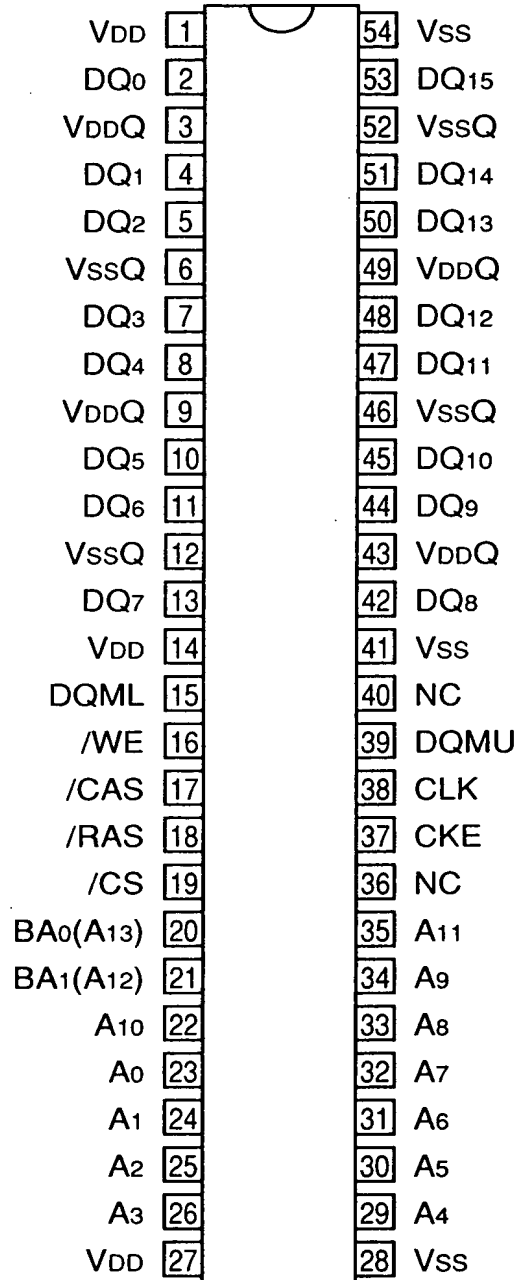


FIG.54 PRIOR ART

TERMINAL NAME	FUNCTION
CLK	MASTER CLOCK
CKE	CLOCK ENABLE
/CS	CHIP SELECT
/RAS	ROW ADDRESS STROBE
/CAS	COLUMN ADDRESS STROBE
/WE	WRITE ENABLE
DQ0~15	DATA INPUT/OUTPUT
DQM(U/L)	OUTPUT DISABLE/WRITE MASK
A0~11	ADDRESS INPUT
BA0,1(A12,13)	BANK ADDRESS
VDD	POWER SUPPLY POTENTIAL
VDDQ	POWER SUPPLY POTENTIAL FOR OUTPUT
VSS	GROUND
VSSQ	GROUND FOR OUTPUT

FIG.55 PRIOR ART

